

Notice of Allowability

Application No.

10/033,705

Applicant(s)

SRINIVASAN ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 10/12/2005.
2. ☒ The allowed claim(s) is/are 1,2,4,6 Renumbered as Claims 1-4.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

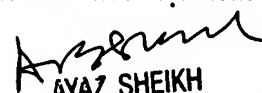
Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Response to Arguments

Claim Rejections - 35 USC § 112

1. Applicant's arguments with respect to Claims 1, 2, 4, 6 and 7 have been fully considered and are persuasive. The rejection 35 USC 112 of Claims 1, 2, 4 and 6 has been withdrawn.

Allowable Subject Matter

2. Claims 1, 2, 4 and 6 are allowed.

3. The following is an examiner's statement of reasons for allowance: The Admitted prior arts [Bachman et al. U.S. Patent 5,097,621, hereinafter "Bach", Peterson, Jr. U.S. Patent 5,857,020], disclose the use of a unique token that is secure from counterfeit and replay attacks and controlling access by a user to content of a storage medium, the content including encrypted data and the means for measuring time, the time clock effectively reaching a reassigned time, to encrypt or decrypt data. Bach discloses a method for a current key to be used to encrypt a message by determining whether the key is valid and generating a new user-unique key (secret key), Peterson discloses applying the public key cryptography to encrypt key k uniquely and storing the key.

However, the admitted prior arts taken independently or in combination, do not disclose, teach or suggest comparing the counter data to reuse criterion wherein the reuse criterion comprises a maximum number of bytes of message data and the counter data comprises a cumulative number of bytes of message data previously sent using an associated reusable secret key.

The present invention provides a method for selecting a current secret key wherein a reuse criterion such as maximum number of messages sent, a cumulative number of messages previously sent or a cumulative number of bytes of message data previously sent, can be used to determine that a new secret key is required. Thus, the present invention further provides a key reuse technique that is robust against system failures, restarts, or other events causing loss of data by comparing counter data with reuse criterion before generating a new secret key.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Art Unit: 2136

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Horace Ng, registration number 39,315, on November 02, 2005.

IN THE CLAIMS:

1. (Amended) In a public key encryption system, a method for selecting a current secret key to be used to encrypt a message, the method comprising:

determining whether a new secret key is required, wherein determining whether a new secret key is required further comprises:

determining whether a previous message has been sent to a recipient;

if a previous message has not been sent to the recipient, determining that a new secret key is required, and

if a previous message has been sent to the recipient:

retrieving counter data from a local data store; and

comparing the counter data to a reuse criterion, wherein the reuse criterion comprises a maximum number of bytes of message data and the counter data comprises a cumulative number of bytes of message data previously sent using an associated reusable secret key;

if the counter data satisfies the reuse criterion, determining that a new secret key is not required; and

if the counter data fails to satisfy the reuse criterion, determining that a new secret key is required;

if a new secret key is required ;

generating the new secret key;

generating a new encrypted secret key by encrypting the new secret key using a public key associated with the recipient of the message;

storing in the local data store the new secret key as a reusable secret key, the new encrypted secret key as a corresponding reusable encrypted secret key, and counter data associated with the reusable secret key; and

selecting as the current secret key the new secret key; and

if a new secret key is not required:

Art Unit: 2136

retrieving from the local data store a reusable secret key and the corresponding reusable encrypted secret key;

updating the counter data associated with the reusable secret key in the local data store;

selecting as the current secret key the reusable secret key;

encrypting the message using the current secret key; and

sending the encrypted message and the encrypted secret key.


7. (Cancelled)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on Tuesday – Thursday 8:00a.m. To 3:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
November 03, 2005.


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100